



**Datuak Babesteko
Euskal Agintaritza**

Autoridad Vasca de
Protección de Datos

Estrategia Corporativa

PLAN ESTRATÉGICO DE LA AVPD



ÍNDICE DEL DOCUMENTO

1	INTRODUCCIÓN.....	6
1.1	MISIÓN.....	6
1.2	VISIÓN	7
1.3	PRINCIPIO DE INDEPENDENCIA	8
2	CONTEXTO PARA LA APLICACIÓN DEL PLAN ESTRATÉGICO.....	11
3	EJE 1 – AUTORIDAD VASCA DE PROTECCIÓN DE DATOS: AUTORIDAD PRO-ACTIVA	17
4	EJE 2 – AUTORIDAD VASCA DE PROTECCIÓN DE DATOS: AUTORIDAD TRANSPARENTE	22
5	EJE 3 – ADECUACIÓN A LA NUEVA LEY DE LA AUTORIDAD VASCA DE PROTECCIÓN DE DATOS	26
6	EJE 4 – ACTUACIÓN EN EL ÁMBITO SECTORIAL	29
7	FACTORES CRÍTICOS DE ÉXITO.....	33

1. Introducción



1 INTRODUCCIÓN

En las últimas décadas se ha repetido en innumerables ocasiones, que en una sociedad tan digitalizada como la actual la adecuada protección del derecho a la protección de datos constituye un factor esencial para que las personas puedan desarrollar su personalidad con libertad. No hace falta subrayar, por tanto, la importancia de dicho derecho.

1.1 Misión

El derecho a la protección de datos de carácter personal es un derecho fundamental autónomo consolidado, tanto en el ordenamiento jurídico como en el ámbito social. Por un lado, normas tan relevantes como el Tratado de Funcionamiento de la Unión Europea (UE), en su artículo 16, como la Carta de Derechos Fundamentales de la UE, en su artículo 8, lo reconocen expresamente. Por otro, resulta evidente que la ciudadanía muestra cada vez mayor interés en la protección de este derecho. No hay más que ver el aumento del número de reclamaciones que se realizan ante las autoridades de control¹ o cómo los medios de comunicación se hacen eco con mayor asiduidad de noticias vinculadas a ese derecho para constatar esta circunstancia. Esto se debe, en gran medida, a que en la actualidad el uso de herramientas como Internet es generalizado. Según el Eustat, en 2022 el 86,3% de la población mayor de 15 años utilizaba Internet con normalidad, aumentando esa cifra al 100% en la franja de edad entre 15 y 24 años. Hoy día no se cuestiona la existencia de este derecho y los debates en torno a esta materia se centran en determinar cuál es su alcance en los diferentes ámbitos. Si esto es así es debido, en gran medida, al trabajo que han realizado las autoridades de control independientes, tanto de sensibilización como de control.

Es misión de la Autoridad Vasca de Protección de Datos (AVPD) proteger a las personas frente el tratamiento que los entes públicos hacen de sus datos. Para ello, la Autoridad desarrolla diversas actividades, a saber: la tutela de derechos, instrucción de expedientes de infracción, difusión de buenas prácticas, asesoramiento a los entes públicos, etc.

¹ En el caso de la Agencia Vasca de Protección de Datos, en el año 2017 las denuncias presentadas fueron 40, mientras que en 2022 fueron 75. En el caso de la Agencia Española de Protección de Datos, por ejemplo, el número de reclamaciones ha aumentado un 46,5% desde el 2020. Memoria AEPD, 2022.



1.2 Visión

En Euskadi el papel de la AVPD ha sido fundamental a lo largo de los años en la consolidación del derecho a la protección de datos. Tras su creación en la Ley 2/2004 de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, es indiscutible que la AVPD ha desarrollado funciones importantes acompañando el proceso de digitalización del sector público, construyendo poco a poco una sólida interpretación, también cuando las normas no eran lo suficientemente precisas, sobre cómo deben tratarse los datos en el ámbito de lo público. Tras la aprobación de nuevas normas generales de protección de datos, tanto en el ámbito europeo, con el Reglamento General de Protección de Datos UE 2016/679 y la Directiva 680/2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, como en el estatal, con la LO 3/2018 de Protección de Datos y Garantía de Derechos Digitales y la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el papel de la AVPD ha sido relevante a la hora de orientar a los entes públicos en la aplicación de dichas normas y de controlar que se cumplen. La labor de la Agencia ha sido de reseñar, si se tiene en cuenta que el nuevo marco normativo venía a cambiar la forma de entender la protección de datos, creando nuevas obligaciones (Registros de Actividades de Tratamiento, Delegados/as de Protección de Datos...) y nuevos derechos que antes no existían o no se reconocían expresamente en las normas (caso del derecho al olvido).

Partiendo de la labor realizada hasta ahora, la Autoridad se plantea como horizonte un escenario en el que las personas son conscientes de la importancia del derecho a la protección de datos, los entes públicos desarrollan buenas prácticas en el tratamiento de datos de carácter personal y generan confianza a la ciudadanía, se respetan los derechos de las personas y en el que la transformación digital de los entes públicos se lleva a cabo con todas las garantías posibles.



1.3 Principio de independencia

El papel de la AVPD como autoridad independiente, garante del derecho fundamental a la protección de datos de carácter personal, se ha visto fortalecido en el nuevo marco regulador, con la atribución de múltiples funciones y potestades. Las opciones de desarrollar todas esas funciones y potestades pasan, A), por adaptar la normativa autonómica de protección de datos, sobre todo la que regula la organización y funcionamiento de la Autoridad, al nuevo marco jurídico y, B), por desarrollar un plan estratégico, que marque las líneas generales de acción de la autoridad de control.

- A) En cuanto a la necesidad de modificar las normas autonómicas de protección de datos se ha aprobado la nueva Ley de Autoridad Vasca de Protección de Datos, que marca los principales criterios sobre los que tendrá que actuar la Autoridad. Junto a la Ley, será importante elaborar una propuesta de Estatuto de la Autoridad, adaptada a las nuevas necesidades que nacen de la aplicación del nuevo marco legal.
- B) En cuanto al Plan Estratégico, constituye una herramienta dirigida, esencialmente, a la ciudadanía, a los entes sobre los que ejerce la función de control la AVPD y a quienes trabajan en la misma. A los/as ciudadanos/as, por ser titulares del derecho a la protección de datos que la Autoridad debe salvaguardar. En este Plan se pretenden articular las principales vías de acción de la AVPD, sobre todo, para sensibilizar a la ciudadanía sobre la importancia de ese derecho y para dar a conocer las herramientas con las que cuenta para controlar activamente lo que sucede con sus datos. A los entes que componen el sector público vasco, por ser los sujetos sobre los que la Autoridad ejerce sus funciones de control y prevención. No se puede olvidar, a pesar de ser una idea repetida, que el sector público trata una gran cantidad de datos en el ejercicio de sus funciones, muchas veces especialmente sensibles. Es fundamental que estos entes respeten el derecho a la protección de datos con el mayor rigor posible. Además de a la ciudadanía y a los entes públicos, este plan estratégico se dirige al personal de la propia AVPD, en la medida en que su cumplimiento exigirá su compromiso con el mismo y su máxima diligencia en el ejercicio de sus funciones.



Tanto la nueva normativa como este Plan Estratégico pretenden reforzar el principio de independencia, que debe tener reflejo, después, en la organización y funcionamiento ordinario de la AVPD. En este sentido, el ente debe tener la capacidad de gestionar sus medios y desarrollar sus funciones con independencia.

2. Contexto para la Aplicación del Plan Estratégico



2 CONTEXTO PARA LA APLICACIÓN DEL PLAN ESTRATÉGICO

En la actualidad, el derecho a la protección de datos se enfrenta a nuevos retos. Esta situación obliga a trazar un plan estratégico, que viene marcado por los distintos factores que caracterizan el contexto en el que actualmente opera el derecho fundamental a la autodeterminación informativa en el sector público. La lectura y aplicación de este plan estratégico debe realizarse al albur de las circunstancias comentadas.

1. El derecho a la protección de datos está viviendo un momento decisivo en la actualidad. En términos generales parece evidente que las nuevas tecnologías siguen desarrollándose a gran velocidad, sin que existan, en muchas ocasiones, herramientas jurídicas bien definidas para afrontar los nuevos retos con garantías. El máximo exponente de esta circunstancia, aunque no el único, pues también podría traerse a colación el debate que plantean los neuro-derechos o el que ofrece el aumento de los ciber-ataques², es la Inteligencia Artificial (IA), conocida desde hace tiempo, pero cuyo uso está adquiriendo nuevas dimensiones los últimos años.

La transformación que se vive a nivel social tiene su repercusión, lógica, en el sector público.

A) En primer lugar, porque esas nuevas tecnologías, cuyo uso se va generalizando, también se incorporan cada vez con mayor frecuencia en la organización y funcionamiento de los entes públicos (no hay más que pensar, por ejemplo, en el uso de la IA en el ámbito médico, con fines predictivos de determinados tipos de enfermedades, o en el uso los diversos sistemas de videovigilancia que pueden utilizarse con fines como la salvaguarda de la seguridad ciudadana, control de tráfico...). El proceso de transformación digital de las Administraciones Públicas sigue su curso y es cada vez más evidente tanto a nivel interno como en las relaciones con la ciudadanía. Si se acude a los últimos datos del Eustat del 2022, se observará que el grado de digitalización en los diferentes niveles del sector público es alto, tanto en relación con los equipamientos como con los procedimientos y

² El BCSC ha puesto de manifiesto este hecho durante los últimos años.



servicios digitalizados. También ha aumentado el uso que se hace por la ciudadanía de esas herramientas, a pesar de que las cifras siguen sin ser especialmente altas.

B) En segundo lugar, porque el proceso de transformación de las Administraciones Públicas se ve afectado por distintos fenómenos, que condicionan e impulsan su desarrollo:

- ✓ primero, porque las circunstancias socioeconómicas, especialmente significativas en el periodo de pandemia de COVID-19, han obligado en los últimos años a consolidar, con mayor o menor alcance, el carácter social del Estado, lo que ha implicado la asunción de más funciones por el sector público dirigidas a proteger a la ciudadanía. Lógicamente, esta circunstancia obliga a tener que prestar nuevos servicios, tramitar nuevos procedimientos y, por consiguiente, a tratar más datos e información;
- ✓ segundo, porque la forma de entender las relaciones jurídico-públicas también ha variado. La ciudadanía cada vez reclama una “mejor Administración”, apelando a ese derecho a la buena Administración que se reconoce en la Carta de Derechos Fundamentales de la UE. Se trataría de una Administración cada vez más cercana, transparente, que fomenta la participación ciudadana y que, necesariamente, debería respetar los derechos subjetivos de las personas, empezando por el derecho a la protección de datos;
- ✓ por último, porque la realidad, cuando se habla de las nuevas tecnologías, es cada vez más compleja, lo que obliga a las administraciones a tener que adaptar su organización a estos cambios. Se crean nuevos órganos administrativos e incluso nuevos entes con personalidad jurídica propia, que responden a un inevitable proceso de especialización de las administraciones públicas. Ejemplo de ello es la reciente creación en Euskadi de la Agencia Vasca de Ciberseguridad (Ley 7/2023). El surgimiento de nuevos entes y órganos administrativos obliga, a su vez, a crear nuevos sistemas de información que posibiliten flujos de datos, tanto intra-administrativos como interadministrativos, ágiles pero seguros.

Este proceso de transformación que en los últimos años se ha acelerado en todos los ámbitos de la vida, también en el sector público, obliga a tener presente, en todo momento, la relevancia del derecho a la protección de datos. Esta idea debe subrayarse, no ya porque



dicho derecho está consolidado en las normas, también a nivel de la UE, sino porque la propia legitimidad social del sector público reclama el respeto de los derechos fundamentales. Esto es especialmente importante en un momento en que la coyuntura política internacional, también se deduce de las estadísticas, refleja una pérdida por la ciudadanía de la confianza en lo público. Evidentemente, la AVPD tiene un papel esencial a la hora de aportar criterios ciertos sobre cómo se deben de tratar los datos en el sector público, a fin de garantizar seguridad jurídica. Esta seguridad constituye condición de posibilidad para que las personas confíen en el buen funcionamiento de las administraciones.

2. Otro factor determinante a la hora de caracterizar el contexto en el que se van a producir los debates sobre la materia de la protección de datos, es la aprobación, durante los últimos años, de nuevas normas sobre la materia, que obligan a la autoridad a analizarlas, interpretarlas y a concretar cómo deben aplicarse. Ejemplo de ello son normas tan relevantes como la LO 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el RD 203/2021, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, el Decreto 91/2023, de Euskadi, de atención integral y multicanal a la ciudadanía y acceso a los servicios públicos por medios electrónicos, o la Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. A estas se sumarán, en un futuro próximo, otras que ya se están tramitando en el ámbito de la UE, vinculadas a materias tan relevantes como la Inteligencia Artificial o la construcción de un Espacio Europeo de Datos Sanitarios. La aplicación de esas normas implica la articulación de nuevos tratamientos de datos que la AVPD debe analizar y sobre los que deberá fijar criterio.

3. Un tercer factor que condiciona la manera de interpretar el contenido y los límites del derecho a la protección de datos en el sector público lo ha puesto de manifiesto la pandemia de COVID-19. La lucha contra la pandemia y sus efectos ha revelado la importancia de contar con un adecuado sistema de tratamiento de datos en el sector público. Primero, porque ha puesto de manifiesto lo importante que es, que el sector público pueda



desarrollar sus funciones y ejercer sus potestades, dirigidas a salvaguardar el interés público, de forma ágil y eficaz, así como la conveniencia de que, para ello, cuente con sistemas de información igual de ágiles y eficaces, con sistemas interconectadas e interoperables. Segundo, porque ha situado en el centro del debate la cuestión de si para llevar a cabo los tratamientos de datos por las administraciones, en el ejercicio de sus funciones, es necesario el consentimiento de las personas titulares de los datos.

El papel de la AVPD resultará esencial a la hora de fijar criterios concretos sobre cómo pueden las administraciones tratar los datos de la ciudadanía en el cumplimiento de sus objetivos, determinados previamente por las normas, y de concienciar a la ciudadanía de que el uso de sus datos por los entes públicos se justifica en la consecución de intereses públicos relevantes.

4. Un cuarto factor a tener en cuenta a la hora de enmarcar los debates actuales sobre protección de datos, es el hecho de que hay sectores que a día de hoy están viviendo una transformación relevante o sobre los que están influyendo de manera especial las nuevas tecnologías, lo que merece un análisis particularizado y que se desarrollen acciones más específicas por la autoridad de control independiente. Se está pensando, por ejemplo, en ámbitos como el sanitario, el de seguridad o educación, que merecen un estudio individualizado. La AVPD tiene un papel especialmente relevante en estos sectores, en la medida en que los datos de la ciudadanía se ven comprometidos de forma particular.



Todos estos factores son esenciales a la hora de comprender el debate actual en torno al derecho a la protección de datos y marcan el campo de acción de la Autoridad Vasca de Protección de Datos para los próximos años. Teniendo en cuenta este contexto, la actuación de la Autoridad se enmarcará sobre cuatro ejes fundamentales: la pro-actividad; la transparencia; la necesidad de adaptarse al nuevo marco jurídico; y, la actuación sobre algunos ámbitos de la realidad especialmente sensibles.



3. Eje 1 – Autoridad Vasca de Protección de Datos: Autoridad Pro-Activa



3 EJE 1 – Autoridad Vasca de Protección de Datos: Autoridad Pro-Activa

El papel de las autoridades de control se ha vinculado la mayoría de ocasiones con el ejercicio de la potestad sancionadora o de tutela de derechos de las personas titulares de los datos, es decir, con acciones que se desarrollan una vez ha habido un tratamiento de datos posiblemente irregular. Estas funciones son fundamentales. Sin embargo, igual de relevantes son las actuaciones que las autoridades de control deben desarrollar *ex ante*, de manera preventiva, antes de que la irregularidad se produzca. Hay que tener en cuenta que la aprobación del RGPD trajo consigo un cambio de paradigma en la forma de proteger los datos de carácter personal, apostando por la pro-actividad, es decir, obligando a los responsables del tratamiento a hacer todo lo posible y a actuar diligentemente en la protección de los datos. Se trata de poner el foco en la adopción de medidas que protejan los datos desde el inicio, desde que se diseñan los sistemas de información. Evidentemente, esto obliga a que desde las autoridades de control se desarrolle una importante tarea de sensibilización, información, asesoría y formación sobre cómo se deben proteger los datos de las personas de manera adecuada, dirigida tanto a la ciudadanía como a los responsables y encargados de tratamiento. Resulta fundamental subrayar el papel que ha tenido a lo largo de los años la AVPD en la sensibilización y formación, tanto de la sociedad, en general, como del sector público, en particular. Si el derecho a la protección de datos cuenta hoy con un reconocimiento generalizado es, en gran medida, por esa labor que ha ido realizando la autoridad de control. Es necesario seguir profundizando en estas funciones teniendo en cuenta los nuevos retos que plantean las nuevas tecnologías. Son tareas que ya realiza la Autoridad, pero a las que debería darse mayor relevancia.



Dentro de las funciones que el Reglamento General de Protección de Datos UE atribuye, en su artículo 57, a las autoridades de control se encuentran, entre otras, “b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento (...); c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y



libertades de las personas físicas con respecto al tratamiento; d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento; i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;"

Estas referencias exigen a las autoridades de control, en concreto a la AVPD, que sean proactivas en la protección de datos de carácter personal. Para ello es necesario que se lleven a cabo diferentes actuaciones, a saber:

A) Actuación 1: formalización de planes de formación y asesoramiento con entes que componen el sector público de Euskadi y que son los principales responsables de tratamiento de datos de carácter personal sobre los que desarrolla sus funciones la AVPD. Se trata de una actividad que ya se desarrolla pero que merece una mayor atención desde la Autoridad. Para ello resulta esencial mantener la relación que ya se tiene con el Instituto Vasco de Administración Pública y fortalecerla, así como articular líneas de acción con los/as Delegados/as de Protección de Datos de los entes que componen el sector público vasco. El objetivo no es, únicamente, llevar a cabo una transferencia general del conocimiento del personal de la AVPD a quienes tienen que tratar los datos desde los entes públicos, sino también asesorar a dichos entes en el diseño y aplicación de los sistemas de información concretos que tienen que utilizar en el ejercicio de sus funciones;

B) Actuación 2: fomento de la actividad investigadora en materia de protección de datos. Tratándose la protección de datos, y en general todo lo que afecta a las nuevas tecnologías, de una materia en constante transformación resulta necesario que desde diferentes agentes se desarrolle tareas de investigación, dedicadas a actualizar el conocimiento sobre esta materia. Más allá de la labor investigadora que se pueda desarrollar desde la propia Autoridad, aportando criterios específicos propios sobre cómo deben interpretarse las normas o/y la jurisprudencia al respecto, será tarea de ésta fomentar la investigación desde los más importantes operadores dedicados a tal fin, caso de las universidades. Es necesario vehicular una relación directa con las universidades vascas, esencialmente con la



Universidad del País Vasco/Euskal Herriko Unibertsitatea, y en concreto con las facultades en las que se imparten títulos, tanto de grado como de posgrado, vinculados a la materia que aquí interesa. Que se realicen Trabajos de Fin de Grado, Trabajos de Fin de Máster y, sobre todo, tesis doctorales sobre la protección de datos es esencial para encontrar aportaciones de interés, con suficiente grado de profundización, que ayuden a avanzar en la mejor aplicación del marco jurídico.

La actividad investigadora también se fomenta con la participación en grupos de trabajo o proyectos de investigación vinculados a materias como la digitalización de las administraciones, la protección de datos o la innovación tecnológica.

Con este mismo fin, cada año se han convocado los importantes premios de la AVPD, que también premian la actividad investigadora. Es necesario que dichos premios tengan un mayor eco en la sociedad, para lo que puede ser de interés otorgarles mayor proyección y dotarlos económicoamente;

C) Actuación 3: potenciación de campañas de sensibilización. A día de hoy la AVPD no opera como un ente desconocido en la sociedad, y es cierto que su labor es puesta en valor por el sector público y es cada vez más conocida por la ciudadanía, en general. Sin embargo, es necesario que desde la Autoridad se fortalezca la función de sensibilización en materia de protección de datos, tanto de la ciudadanía como de los entes responsables de los tratamientos de datos. En el caso de la ciudadanía, para que sea consciente de la relevancia del derecho fundamental a la protección de datos, para conocer su contenido y las herramientas con las que cuenta para su protección. También, para que tenga constancia de que las administraciones emplean sus datos de acuerdo con las normas, con fines concretos de interés público y con todas las garantías. En el caso de los responsables del tratamiento de datos, para tomar conciencia de lo importante que es el respeto del derecho a la protección de datos de las personas, no ya para cumplir con las normas, sino también para legitimar socialmente el sector público. En este sentido, resulta imprescindible:

- ✓ por un lado, una relación constante, no únicamente cuando surjan problemas puntuales de interés social, con los medios de comunicación;
- ✓ por otro, es necesario el uso de las redes sociales por parte de la Autoridad para llegar a la ciudadanía de una manera eficaz;



- ✓ por último, también será fundamental la organización de eventos, seminarios o congresos, dirigidos a sensibilizar, sobre todo, a quienes tratan los datos de la ciudadanía, así como la participación en foros creados al efecto;
- ✓ más allá de las campañas de sensibilización que se puedan realizar destinadas a la sociedad, en general, será necesario hacer especial hincapié en las campañas dirigidas a menores de edad, no ya para que pongan en valor su derecho a la protección de datos y para que aprendan a proteger ese derecho en Internet, sino para que aprendan a realizar un buen uso de las nuevas tecnologías.

D) Actuación 4: creación de canales de comunicación rápidos y seguros con los entes que componen el sector público vasco y sus respectivos/as Delegados/as de Protección de Datos, para actuar de una manera ágil y eficaz, por ejemplo, ante posibles violaciones de seguridad. Será necesario articular, mediante sede electrónica o cualquier medio electrónico, herramientas para dar a conocer la AVPD y relacionarse con ella.

E) Actuación 5: aprobación de circulares, códigos de conducta e instrucciones que ayuden a interpretar las normas de protección de datos, sobre todo en el ámbito sectorial, a fin de garantizar la seguridad jurídica tanto de la ciudadanía como de quien tiene que aplicar esas normas.

La consolidación de una Autoridad proactiva en la salvaguarda del derecho a la protección de datos es esencial en un momento en que la normativa sobre la materia reclama a los responsables de tratamiento de datos actuar de manera preventiva, desde el diseño, en la protección de datos.

4. Eje 2 – Autoridad Vasca de Protección de Datos: Autoridad Transparente



4 EJE 2 – Autoridad Vasca de Protección de Datos: Autoridad Transparente

Es fundamental que la AVPD tenga visibilidad en la sociedad, que sea un ente accesible para las personas y que, además, tanto su funcionamiento y organización, así como todas las decisiones que se adoptan y que tengan interés social, sean conocidas por la ciudadanía. Se trata de hacer efectivo el derecho a la buena administración reconocido en la Carta de Derechos Fundamentales de la UE, aplicado a la Autoridad, desarrollando diferentes actuaciones.



A) Actuación 1/Visibilidad: uno de los factores más relevantes para que la AVPD pueda desarrollar las funciones que más arriba se han comentado, esencialmente de sensibilización y formación, es que sea conocida en los ámbitos de la sociedad en que dichas funciones se van a desarrollar.

- ✓ Primero, en la sociedad, en general, a fin de que la ciudadanía tome conciencia de su existencia y de sus funciones. Para ello, es necesario dar un impulso a las distintas herramientas que pueden dar a conocer a la autoridad de control (redes sociales, medios de comunicación, página web).
- ✓ Segundo, en las administraciones, para que tengan conocimiento de qué criterios deben seguir en el tratamiento de datos de carácter personal, cuáles son las mejores prácticas en este sentido, así como para crear vías rápidas de comunicación para resolver dudas, realizar observaciones, dar a conocer situaciones concretas en que se puedan ver comprometidos los derechos de las personas, etc.
- ✓ Tercero, en entidades que desarrollan actividades de especial interés en materia de protección de datos. Se está pensando en las universidades o, también, en corporaciones de derecho público como los colegios profesionales.

B) Actuación 2/Accesibilidad: una “buena” administración independiente pasa porque los servicios que presta sean accesibles para los usuarios y las usuarias. Es necesario crear las herramientas adecuadas para que la ciudadanía y los entes que deben cumplir con la normativa de protección de datos accedan de manera sencilla y ágil a esos servicios y a los



procedimientos que se pueden tramitar ante la Autoridad, a documentos normalizados para que puedan ejercer sus derechos, a los dictámenes, guías y resoluciones, etc.

C) Actuación 3/Transparencia: una de las máximas que ha de cumplir la AVPD, tal como venía haciendo, es la de la transparencia. Hay que tener en cuenta que la autoridad de control independiente presta un servicio esencial en una materia tan relevante como es la protección de un derecho fundamental en el sector público. En este sentido, la obligación de cumplir con el principio de transparencia deriva de distintos aspectos, a saber:

- ✓ primero, por tratarse de una Administración independiente, que debe guardar, precisamente, la apariencia de esa independencia y neutralidad. No hay mejor mecanismo para ello que la ciudadanía, en términos generales, y las administraciones, en particular, conozcan la organización y funcionamiento de la Autoridad. Es necesario que se conozca su política de gastos, tal como se ha venido haciendo hasta ahora, sus ingresos, la actividad que desarrollan las distintas áreas que componen la entidad, etc. Resultará esencial, a su vez, la transparencia sobre la actividad de la presidencia del ente, a fin de que pueda controlarse su independencia y neutralidad, con acciones como la publicación de su Agenda a través de la implantación de un portal de transparencia;
- ✓ segundo, por tratarse de un ente cuya actividad esencial tiene efectos sobre la ciudadanía. La interpretación de las normas, la resolución de consultas, la tramitación de procedimientos sancionadores, las campañas de sensibilización, la formación, etc. son actuaciones que inciden directamente sobre las personas. Ello obliga a que la Autoridad desarrolle su actividad, en general, de cara a la ciudadanía, publicando activamente las decisiones que toma, los dictámenes, las guías que pueda aprobar, los informes que pueda emitir, etc.

Para que estas tres características (visibilidad, accesibilidad y transparencia) se hagan efectivas será necesario actuar sobre diferentes herramientas o ámbitos, a saber: sobre la página web de la institución, para que sea más intuitiva y accesible; sobre la sede electrónica, que deberá ser de fácil uso para que puedan tramitarse los procedimientos pertinentes con facilidad; sobre las redes sociales que la autoridad independiente debe



utilizar para llegar a la ciudadanía; sobre los medios de comunicación, con los que deberán articularse vías de relación rápidas.



5 EJE 3 – Adecuación a la Nueva Ley de la Autoridad Vasca de Protección de Datos

Teniendo en cuenta que en el Parlamento Vasco se ha aprobado la nueva Ley de la Autoridad Vasca de Protección de Datos, será preceptivo replantearse el papel, la organización y funcionamiento de la, hasta ahora, Agencia Vasca de Protección de Datos. Hay aspectos que van a tener que tomarse en consideración, a saber:



1. En el ámbito interno, como se detallará más abajo, van a tener que replantearse elementos como el organizativo. En la medida en que en la nueva Ley se amplía el ámbito de aplicación, tanto subjetivo como objetivo, de la misma, el campo de acción de la Autoridad también se ampliará. A su vez, se subrayan funciones que anteriormente no habían tenido tanta relevancia, caso de la formación o la acción exterior de la entidad. Siendo así, será necesario establecer, *ad intra*, criterios de funcionamiento que posibiliten a la autoridad llegar a todas las áreas de acción que marca la nueva Ley. En este sentido, se pueden destacar acciones como la reestructuración de la RPT, la revisión de las monografías o la provisión de puestos de trabajo, entre otras.
2. En lo concerniente a la actuación de la AVPD que afecta directamente a la ciudadanía, la nueva Ley llevará a la autoridad a desarrollar tareas de relevancia. Es el caso, fundamental, de la aprobación de circulares o de la realización de auditorías en sectores estratégicos. Se trata de funciones que condicionarán directamente la aplicación por los responsables de tratamiento de las normas de protección de datos, con lo que la Autoridad deberá ejercer sus potestades con rigor. Para ello, será muy relevante dar a conocer la nueva dimensión que adquiere el papel de la Autoridad Vasca, de acuerdo con la nueva Ley.
3. En la medida en que la actividad de la AVPD va a desplegarse también sobre entes a los que se aplica el Derecho privado y a los que se va a poder sancionar económicamente, será necesario establecer criterios concretos de dosimetría de dichas sanciones para



salvaguardar el principio de proporcionalidad que informa el ejercicio de la potestad sancionadora.

6. Eje 4 – Actuación en el Ámbito Sectorial



6 EJE 4 – Actuación en el Ámbito Sectorial

Más allá de la actividad ordinaria de la Autoridad, se considera necesario realizar una actividad específica en sectores concretos, especialmente sensibles, sobre los que la propia ciudadanía ha demostrado un interés particular.



1. En primer lugar, el sector sanitario. Estos últimos años, fundamentalmente después de la pandemia, se ha demostrado la relevancia del tratamiento de datos de salud en la vida cotidiana de las personas. Ya antes la ciudadanía mostraba especial interés en este ámbito, planteando preguntas, ejerciendo derechos como el de acceso a la Historia Clínica, solicitando procedimientos de tutela de sus derechos... A día de hoy hay tres aspectos, esencialmente, que obligarían a realizar una actuación específica sobre los responsables que tratan datos en este ámbito:

- ✓ primero, el hecho de que el proceso de digitalización del sistema sanitario vasco se siga desarrollando. Más allá de los retos ordinarios que plantea todo proceso de este tipo, hay realidades que plantean retos específicos. Por un lado, como se ha apuntado más arriba, la creación del espacio europeo de datos sanitarios, al hilo de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios de 2022, afectará a la gestión de la información del sistema sanitario vasco, en la medida en que implicará nuevos tratamientos de alcance, como son las comunicaciones de los datos a otros países. Por otro, se están desarrollando proyectos desde el sistema sanitario vasco aplicando tecnologías de inteligencia artificial, que requerirán de estudios concretos y pormenorizados.
- ✓ segundo, la posibilidad de que la Autoridad entre a controlar el tratamiento de datos llevado a cabo por entes privados que prestan el servicio sanitario. Teniendo en cuenta que la nueva Ley de la Autoridad Vasca de Protección de Datos amplía su ámbito de aplicación, siendo aplicable a “las personas físicas o jurídicas, si el tratamiento se lleva a cabo para el ejercicio de funciones públicas en materias que sean competencia de las Administraciones Públicas enumeradas en la letra a”, así como a “las entidades de derecho privado que



prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, en lo que respecta a los tratamientos cuya finalidad se encuentre vinculada a la prestación de dichos servicios”, puede interpretarse que la autoridad de control podrá ejercer sus funciones y potestades más allá del servicio público de salud, teniendo en cuenta que, como indica la Ley de Ordenación Sanitaria de Euskadi, “las estructuras sanitarias que no dependan directamente de la Comunidad Autónoma de Euskadi y operen en su ámbito territorial” tienen la consideración de “servicio de interés público” (art. 29);

✓ tercero, el hecho de que todavía, a día de hoy, hay aspectos en el tratamiento ordinario/rutinario de datos sanitarios que deben mejorarse (accesos ilegítimos a historias clínicas, comunicación de datos sanitarios para justificar bajas en administraciones, etc.) y adaptarse a lo que indica la jurisprudencia reciente sobre, por ejemplo, el acceso por las policías a las historias clínicas (STS 971/2022, 16 de diciembre de 2022). Desde la autoridad de control deben aportarse criterios certeros sobre cuáles son las mejores prácticas al respecto de esas cuestiones, que todavía hoy plantean dudas.

2. En segundo lugar, podríamos referirnos al proceso de transformación digital de las administraciones, que todavía se está llevando a cabo y que plantea retos de importancia desde la perspectiva de la protección de datos de carácter personal. Ejemplo paradigmático lo constituye la interoperabilidad y el alcance que puede tener el derecho a no presentar datos y documentos que obran en poder de las administraciones, aplicando la interoperabilidad, en la mayoría de ocasiones, cuando el ejercicio de ese derecho y el flujo de datos entre entes públicos puede darse en perjuicio de un ciudadano o ciudadana (aspecto que ha sido analizado en alguna sentencia polémica del TS recientemente). Más allá de este aspecto, podrían citarse también como acciones de especial relevancia las que tienen que ver con las materias de Ciberseguridad e Inteligencia Artificial. La primera, porque se trata de un fenómeno que cada vez afecta más a los entes públicos. La segunda, porque cada vez son más los entes que utilizan esta tecnología en el desarrollo de sus funciones.



3. En tercer lugar, debería incidirse en el ámbito de la educación. Debe tenerse en cuenta, en este sector, una doble perspectiva. Por un lado, ya se ha indicado que la sensibilización de los/las menores de edad debe constituir un eje fundamental de la actuación de la Autoridad. Para ello, y también para impulsar una formación adecuada de los/las menores de edad, del profesorado y de los padres y madres, en el uso de las nuevas tecnologías, será necesario adoptar una serie de medidas: primero, desarrollar instrumentos de colaboración con los centros educativos para fomentar los planes de formación antedichos; segundo, crear material accesible y sencillo dirigido a los centros educativos, con los criterios generales que los/las menores deben seguir en el uso de las nuevas tecnologías. Por otro, no se puede ser ajeno a la realidad de que, desde los centros de enseñanza, también universitaria, cada vez se está acudiendo más a prestadores de servicios de la sociedad de la información privados, a fin de que se puedan utilizar sus herramientas o aplicaciones con los más diversos fines (uso de repositorios de documentos, herramientas para realizar videoconferencias, servicio de correo electrónico, etc.). Este tipo de operaciones deben respetar las garantías necesarias para que las empresas que prestan ese servicio salvaguarden el derecho a la protección de datos de carácter personal.

4. Por último, resulta de especial interés el análisis de la protección de datos en el ámbito de la seguridad, haciendo especial hincapié en el uso de las videocámaras con ese fin. La nueva Ley da pie a que la Autoridad Vasca de Protección de Datos pueda actuar en este ámbito. No se puede obviar el hecho de que las videocámaras se emplean cada vez más, como instrumentos de seguridad, pero que ese uso debe estar sujeto a criterios específicos. A falta de un marco jurídico claro, sobre todo tras la entrada en vigor de la LO 7/2021 de protección de datos en el ámbito penal, que también regula el uso de videocámaras, es necesario que se aporte cierta seguridad jurídica, tanto a quienes deben utilizar esas herramientas en el ejercicio de sus funciones como a la ciudadanía. Esta necesidad viene reforzada por el hecho de que cada vez son más las videocámaras que se utilizan con fines de seguridad, y porque las cámaras utilizadas cada vez incluyen tecnologías más avanzadas, caso de las “body cams” o las pistolas que incorporan videocámaras.

7. Factores Críticos de Éxito



7 FACTORES CRÍTICOS DE ÉXITO

La tarea de las autoridades de control para hacer frente a todos estos retos es esencial. Contar con una Autoridad de protección de datos propia en Euskadi garantiza que los objetivos planteados, sobre todo en el ámbito del sector público, puedan llevarse a cabo de manera más precisa y eficaz, desde la cercanía, teniendo en cuenta las particularidades que presenta nuestro sector público.



Primero, porque se cuenta con un marco jurídico propio, que reclama de un análisis particularizado y una aplicación especializada, que, evidentemente, puede hacerse con mayor rigor desde una entidad propia. Piénsese en la Ley Vasca del Sector Público o en la Ley Vasca de Potestad Sancionadora, que, evidentemente, se analizan con una visión más cercana desde una entidad propia.

Segundo, porque la intervención de la AVPD se lleva a cabo en sectores gestionados en base a competencias propias. Piénsese en ámbitos tan sensibles como la sanidad, la educación, el tributario, incluso la seguridad. Evidentemente, en estos ámbitos el tratamiento de datos genera una preocupación social especial. En la medida en que dichos sectores se gestionan desde entidades vascas (sea Gobierno Vasco, entidades forales o municipales, o sector público institucional) resulta imprescindible que desde una autoridad



independiente propia se atienda a las particularidades que presenta esa gestión, marcando criterios específicos, basados en las necesidades dichos entes.

Tercero, porque las funciones a desarrollar por la AVPD tienen que adecuarse a necesidades de las administraciones vascas, como puede ser, por ejemplo, el prestar un servicio en las dos lenguas oficiales. Teniendo en cuenta que desde la Autoridad deben desarrollarse tareas de formación, comunicación, sensibilización, etc., es fundamental contar con una entidad capaz de relacionarse tanto en euskera como en castellano.

Cuarto, porque en la medida en que tanto la regulación de la protección de datos de carácter personal como los propios tratamientos de los datos se desarrollan en esferas internacionales, esencialmente en la UE, es fundamental contar con una presencia en ese ámbito que salvaguarde los intereses de las administraciones vascas en esta materia.

Debido, precisamente, a la importancia de contar con una Autoridad propia resulta esencial adoptar medidas dirigidas a fortalecer su papel como garante del derecho a la protección de datos en el ámbito de Euskadi. Para ello deberán adoptarse diferentes medidas.



1. La acción principal que se deberá desarrollar será la impulsión de un nuevo Estatuto de la Autoridad, adaptado a la nueva normativa europea y estatal, que derogue el actual Estatuto de 2005.



2. Será necesario seguir mejorando las competencias de la institución para responder con garantías a los retos que plantea la realidad. En este sentido, será esencial la actualización constante del conocimiento en materia de nuevas tecnologías y protección de datos, teniendo que articular planes internos de formación.

3. Será necesario dotar de los suficientes recursos a la institución para poder desarrollar con eficacia todas las funciones que se le atribuyen en las normas vigentes y las que se puedan aprobar en el ámbito autonómico, estatal o internacional:

- ✓ estabilización y ampliación de la plantilla,
- ✓ dotar de recursos económicos suficientes en los presupuestos,
- ✓ dotar de infraestructuras y equipamiento adecuado: la necesidad de contar con la independencia suficiente para la realización de sus funciones exige que la capacidad de auto-organización de la Autoridad se pueda aplicar en la organización de la sede y en la gestión de recursos.

4. Resultará fundamental plantear en el ámbito interno de la AVPD la articulación de un sistema adecuado para desarrollar la tarea de formación, ya sea desde el área jurídica e inspección o creando un órgano específico para ello.

5. Resulta conveniente plantearse la necesidad de configurar y desarrollar la sede electrónica de la AVPD y el registro electrónico, atendiendo a un plan de modernización específico, que se ajuste a las necesidades del ente. Esto podría facilitar la relación y la comunicación con la ciudadanía y con los/as responsables de tratamiento de datos.

6. Es necesario fortalecer el trabajo en equipo que se hace en la Autoridad. Garantizar un entorno y unas condiciones de trabajo adecuadas; puesta en común del conocimiento entre el personal; atender a las necesidades que se plantean desde las diferentes áreas que componen la Autoridad. Teniendo en cuenta la tipología del trabajo que se desarrolla en la APVD, esencialmente la redacción de informes, resoluciones, dictámenes, etc., es necesario que se pueda llevar a cabo de la forma más cómoda para las empleadas y los empleados, adoptando medidas orientadas a impulsar la productividad del personal de la Autoridad.



7. En el desarrollo de sus tareas la organización de la AVPD tiene que mirar también hacia fuera. Primero, porque todas sus funciones deberán desarrollarse de acuerdo al principio de cooperación con los entes que componen el sector público vasco. Segundo, porque desde la propia Autoridad deben fomentarse herramientas de colaboración entre esos entes, a fin de que comparten buenas prácticas en materia de protección de datos. Gran parte de las potestades que debe ejercer la autoridad de control debe realizarlas en cooperación con otros entes. En primer lugar, es necesario seguir fortaleciendo, como se ha hecho hasta ahora, la relación con las demás autoridades de control, tanto la estatal como las demás autonómicas existentes. Es esencial la comunicación entre las autoridades de protección de datos a fin de fijar criterios comunes ante problemas de la misma entidad. Es fundamental, también, la acción conjunta entre las distintas autoridades en sectores concretos que plantean problemáticas particulares, como puede ser el sanitario. En segundo lugar, es importante la relación entre la AVPD y otros entes que también han contado con un papel relevante en materia de protección de datos o de digitalización del sector público. Es el caso del Ararteko, teniendo en cuenta que los últimos años ha demostrado una preocupación particular y reforzada sobre la cuestión de la Administración Electrónica, pero también de otros entes que se dedican a asistir a las administraciones en los procesos de digitalización, caso de BiscayTIK, por ejemplo. En tercer lugar, resultará fundamental, para fomentar la labor investigadora en materia de protección de datos, la relación de la Autoridad con el sistema universitario vasco. Por último, será importante, para seguir desarrollando la labor de formación que la AVPD ha venido realizando, consolidar su relación con el Instituto Vasco de Administración Pública (IVAP-HAEE), teniendo en cuenta su papel relevante en este ámbito.

8. Elaboración del plan de modernización y del plan de normalización del uso del euskera para la AVPD, y articulación de los medios, tanto personales como técnicos, necesarios para llevarlos a cabo.

En términos generales, se puede entender que en la medida en que mejora la organización y funcionamiento de la AVPD (capacidad de autoorganizarse, más medios, más formación del personal, mayor y mejor digitalización, mejores canales de comunicación con la ciudadanía, con los/as DPDs y responsables de tratamiento) mejor se podrá aplicar el Plan



Estratégico, lo que repercutirá en una mayor sensibilidad de la ciudadanía y del sector público en materia de protección de datos. De ello resultará una mejor prevención en la protección del derecho, evitando que se produzcan prácticas contrarias a Derecho.

El grado de cumplimiento del Plan Estratégico deberá cuantificarse periódicamente. Para ello, cada área de trabajo deberá emitir anualmente un informe en el que se determinen los avances que se han hecho en el cumplimiento del Plan, así como las posibles propuestas de mejora del mismo.